



2 Marylebone Road
London
NW1 4DF
which.co.uk

Financial Conduct Authority
12 Endeavour Square
London
E20 1JN

Which? response to the Call for input - Consumer Investments

Summary

- Online platforms are playing a growing role in enabling scammers to reach and defraud victims and yet have no legal obligations to prevent scam content on their sites.
- The risk-based approach to scam adverts currently taken by online platforms is no longer adequate to address fraud in online promotions. Which? believes that there is a strong case for regulation of advertising on online platforms which is underpinned by the precautionary principle.
- Fundamental to addressing scams online will be introducing legally enforceable responsibilities that apply to online platforms as communicators of adverts to have in place measures for prevention of scams, better and faster reaction to reported scams, more transparency, and oversight by relevant authorities.

Introduction

Which? welcomes the opportunity to respond to this Call for Input which provides an important forum to consider how consumers can be empowered to invest with confidence and be better protected from scams on online platforms. As the importance of the digital world continues to grow in our everyday lives, it is vital that consumers can continue to make the most of the many opportunities this transformation presents. While this Call for Input is an important forum for discussing the ways of addressing the issue of fraudulent adverts for investments on online platforms, Which? is concerned about the broader lack of regulatory oversight and responsibility of online intermediaries. Therefore, our response addresses the following questions:

- Q33: How can people be better protected from scams?
- Q34: What are the most suitable and proportionate remedies to further tackle scams and other online investment harms?

Online scams

Online platforms bring huge benefits for consumers in the form of greater choice, convenience, and lower costs. The services provided by online platforms are now an essential part of daily life, allowing people to shop, socialise, and work with greater ease than ever. This reliance on digital services has increased significantly as a result of the coronavirus pandemic. However, there is significant evidence that the lack of clear legal responsibilities on platforms to ensure the safety of their users has left consumers increasingly exposed to fraud, safety risks, and misleading information from the content hosted on these sites.

Online platforms, including social media sites and search engines, are playing a growing role in enabling criminals to reach and defraud internet users. Action Fraud estimates that in the year to June 2020, 85% of all fraud was cyber-enabled and that the use of social media is increasing in all

aspects of fraud.¹ Our investigations have found that prominent types of online scams target those who are looking for investments, insurance, pension advice, online shopping, and even those seeking debt help. Recent Which? investigations have uncovered impersonator ads appearing in Google search results for insurance and investment firm Aviva,² financial technology company Revolut,³ and debt charity StepChange. Action Fraud figures show the total number of fraud reports they received in the year to June 2020 was 822,276 and the value of losses from reported incidents was £2.3 billion.⁴ It is particularly concerning that the number of reported investment-related scams have quadrupled since July.⁵ Therefore, we share the FCA's concern that despite all the efforts made by various stakeholders, too many consumers are still falling victim to scams.

The gap in consumer protection from scams on online platforms

Online fraud is a very broad area, and Which? is calling for the government to take a holistic approach to tackling scams through Online Harms regulation. However, tackling scam adverts for financial products on online platforms should be given immediate priority, given the speed and the number of consumers that an online ad can reach instantly across borders.

The current advertising rules and the regulation of financial promotions do not protect consumers from fraud. The self-regulatory rules on non-broadcasting advertising in the UK are effective when advertisers have an interest in maintaining their good reputation. However, the rules outlined in the CAP Code apply to advertisers and not to online platforms. This creates an incentive for legitimate and reputable brands to comply, but criminals do not give regard to self-compliance and rules. The rules mean little to them if they can continue to post potentially fraudulent adverts without background checks or verification.

The Code also does not address ads that originate from overseas. These ads, despite being targeted at UK consumers, are subject to the jurisdiction of the relevant authority in the country from which they originate.⁶ Consumers in the UK have no information about where those 'companies' that are advertising come from, which creates an information asymmetry between consumers and advertisers, and could have an effect on consumer decision making.

Initiatives by online platforms that aim to verify the identity of advertisers and, in some cases, their business operation models, are a step in the right direction. However, we are concerned that they do not always complete the verification before ads go live. These policies are not legally binding and their enforcement is not monitored by regulators.

Under the eCommerce Directive⁷, search engines and other hosting providers are currently required to remove fraudulent adverts 'expeditiously' once they have been made aware of them. However no

¹ Action Fraud, Fraud Crime Trends 2019–20, 2020, Available at: <https://data.actionfraud.police.uk/cms/wp-content/uploads/2020/07/Fraud-crime-trends.pdf>

² Which?, How scammers use Google to lure victims, September 2020, Available at: <https://www.which.co.uk/news/2020/09/browser-beware-how-scam-advertisers-use-google-to-lure-their-victims>

³ Which?, Google fails to stop scam ad targeting Revolut users for a third time, September 2020, Available at: <https://www.which.co.uk/news/2020/09/google-fails-to-stop-scram-ad-targeting-revolut-users-for-a-third-time/>

⁴ Action Fraud, Fraud Crime Trends 2019–20, 2020, Available at: <https://data.actionfraud.police.uk/cms/wp-content/uploads/2020/07/Fraud-crime-trends.pdf>

⁵ With losses of £9.4m to 12 October 2020. Source: Coronavirus: Investment scams quadruple since virus lockdown, Available at: <https://www.bbc.co.uk/news/business-55126228> (accessed on 10 November 2020)

⁶ Plum Consulting on behalf of the e Department for Digital, Culture, Media & Sport, Mapping online advertising issues and the industry and regulatory initiatives addressing them, May 2020, Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/898866/Mapping_online_advertising_issues_and_the_industry_and_regulatory_initiatives_aimed_at_addressing_them.pdf

⁷ The eCommerce Directive is mainly transposed in the UK by the Electronic Commerce (EC Directive) Regulations 2002. However, financial services elements are transposed by the Electronic Commerce Directive (Financial Services and Markets) Regulations 2002, Article 72A of the Financial Services and Markets Act (Regulated Activity) Order 2001, and Article 20B of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005.

timeframe is given for this. If they do so, this exempts them from liability. The case by case notice and takedown approach - especially for online adverts - is overly reactive and is no longer adequate to protect consumers. We believe this is due to the following:

- 1) An online ad can instantly reach a large number of consumers within a very short period of time. This leaves a potentially fraudulent ad live, promoted to large audiences without the assurance that it is posted by a legitimate advertiser. It can take considerable time from when the potentially fraudulent ad is published to the moment when it is removed by the platform. For instance, in September, a scam ad targeting Revolut users remained live for five days after we reported it to Google, despite it being the third occasion we had flagged fraudulent Revolut adverts on the site.⁸
- 2) This approach relies on consumers to recognise and report the scam ad. By their nature, these ads can be very convincing, so it cannot be reasonably expected from an average consumer to be able to spot a scam. A third of participants in a Which? online research community of Facebook users did not know that fake products might be advertised on social media sites while a quarter did not recognise an investment scam advert with a fake endorsement from a celebrity.⁹ Alongside this limited awareness, Which? found that research participants were often overconfident in their ability to recognise scam content and that there was no correlation between participants' confidence in their ability to spot scams and their actual ability. This combination of limited awareness and overconfidence leaves people at risk of falling victim to fraud.
- 3) Organic, user-generated scam content, which is extremely easy to find on social media platforms is not addressed. Our investigations have uncovered scammers openly selling personal information that has been captured illegally on Facebook, Instagram and Twitter. Which? was able to find 50 scam profiles, pages and groups on the sites promoting the sale of a mixture of stolen identities, credit card details and compromised accounts.¹⁰

Therefore, Which? agrees with the FCA that online scams should be included within scope of the Online Harms regulation. Which? argues that this should cover scams related to financial products but also other types of scams online - such as purchase scams, sale of stolen consumer data which can enable scams, fraudulent organic content and other types of evolving fraudulent practices more broadly.

Recommended solutions

Given the extent of the threat from online scam adverts and promotions, there is a need for regulatory interventions led by a precautionary approach to financial promotions and other adverts for financial services, products and financial advice. The hosting providers must take measures to prevent scams, be more responsive to remove them when they are made aware of them, be more transparent to consumers and accountable to regulators.

Prevention

Which? believes that online platforms must ensure that advertisers are legitimate before their ads go live, as a minimum. They must take proactive steps and conduct due diligence through Know Your Business Customer schemes and ensure that any financial promotion which they communicate has first been approved by an authorised person or otherwise falls within the scope of an exemption in

⁸ Which?, Google fails to stop scam ad targeting Revolut users for a third time, September 2020, Available at: <https://www.which.co.uk/news/2020/09/google-fails-to-stop-scram-ad-targeting-revolut-users-for-a-third-time/>

⁹ Which?, Connecting the world to fraudsters?, October 2020, Available at: <https://www.which.co.uk/policy/digital/6514/connectingfraudsters>

¹⁰ BBC, Facebook and Twitter allow scammers 'free rein', 2020, Available at: <https://www.bbc.co.uk/news/technology-52471837>

the Financial Promotions Order. They should also prevent already identified user-generated fraudulent content from reappearing.

Better and faster reactive measures

In the event fraudulent content does make it onto the sites, then there needs to be faster action from online platforms to take the scam ads down and prevent them from reappearing in a slightly different form after the original advert is removed. When the platform is aware of the potential fraudulent activity, it must be legally required to report these cases to the relevant enforcement authorities. Furthermore, there should be a legal requirement for online platforms to have regard to the FCA's Warning List and block those companies listed on it from advertising financial products on their sites.

Transparency

The important information about the advertisers and the ads on online platforms must be displayed in a user-friendly way. We would like the FCA to explore how this transparency can be delivered in the most useful way for consumers, including:

- Transparency about the level of checks performed on the advertisers and their ads
- If consistent labelling of adverts for financial products and services across digital platforms would improve consumer decision-making

Online platforms should also be required to be transparent about their actions against fraudulent activities and regularly publish public reports on how they enforce the terms and conditions for advertising and community standards.

Stronger regulatory oversight

We believe there is a strong case to include fraud within Online Harms legislation, given the FCA's limited power to take down advertising and user-generated content by those seeking to scam people via online platforms. Alternatively, the government should review the regulation on electronic commerce to update the legal responsibilities of online platforms - 'information society service providers' - to empower regulators to introduce additional measures for online platforms for fraud prevention.

About Which?

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good, here to make life simpler, fairer and safer for everyone. We're the independent consumer voice that provides impartial advice, investigates, holds businesses to account and works with policymakers to make change happen. We fund our work mainly through member subscriptions. We're not influenced by third parties – we never take advertising and we buy all the products that we test.

For further information please contact Senka Andjelkovic, Policy Adviser, at

senka.andjelkovic@which.co.uk.

15 December 2020